The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/02/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird, the most severe of which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 78.0
- Mozilla Firefox ESR prior 68.10
- Mozilla Thunderbird versions prior to 68.10.0

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Thunderbird, the most severe of which could allow for remote code execution. These vulnerabilities can be exploited if a user visits a specially crafted web page. Details of these vulnerabilities are as follows:

- A VideoStreamEncoder may have been freed in a race condition with VideoBroadcaster::AddOrUpdateSink, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. (CVE-2020-12416)

- Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash.Note: this issue only affects Firefox on ARM64 platforms. (CVE-2020-12417)
- Due to confusion processing a hyphen character in Date.parse(), a one-byte out of bounds read could have occurred, leading to potential information disclosure. (CVE-2020-12425)
- During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. Note: An unmodified Firefox browser does not generate RSA keys in normal operation and is not affected, but products built on top of it might. (CVE-2020-12402)
- Memory safety bugs present in Firefox 77. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-12426)
- In non-standard configurations, a JPEG image created by JavaScript could have caused an internal variable to overflow, resulting in an out of bounds write, memory corruption, and a potentially exploitable crash. (CVE-2020-12422)
- Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. (CVE-2020-12418)
- When %2F was present in a manifest URL, Firefox's AppCache behavior may have become confused and allowed a manifest to be served from a subdirectory. This could cause the appcache to be used to service requests for the top level directory. (CVE-2020-12415)
- When constructing a permission prompt for WebRTC, a URI was supplied from the content process. This URI was untrusted, and could have been the URI of an origin that was previously granted permission; bypassing the prompt. (CVE-2020-12424)
- When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. (CVE-2020-12421)
- When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. (CVE-2020-12419)
- When the Windows DLL "webauthn.dll" was missing from the Operating System, and a malicious one was placed in a folder in the user's %PATH%, Firefox may have loaded the DLL, leading to arbitrary code execution. Note: This issue only affects the Windows operating system; other operating systems are unaffected. (CVE-2020-12423)
- When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. (CVE-2020-12420)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Mozilla to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

Mozzilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-26/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12402
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12415
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12417
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12418
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12419
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12420
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12421
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12422
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12423
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12424
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12425
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12426